Journal of Algebra **231,** 374–386 (2000)
doi:10.1006/jabr.2000.8371, available online at http://www.idealibrary.com on IDEAL®

Finite Simple Groups of Bounded Subgroup Chain Length

K. Alladi

R. Solomon[1]

Department of Mathematics, Ohio State University, Columbus, Ohio 43210
E-mail: solomon@math.ohio-state.edu

and

A. Turull[2]

Department of Mathematics, University of Florida, Gainesville, Florida 32611
E-mail: turull@math.ufl.edu

Communicated by R. Steinberg

Received November 15, 1999

Given a finite group G, we denote by $l(G)$ the length of the longest chain of subgroups of G. We study whether certain sets of non-isomorphic finite simple groups S with bounded $l(S)$ are finite or infinite. We prove, in particular, that there exists an infinite number of non-isomorphic non-abelian finite simple groups S with $l(S)$ bounded. © 2000 Academic Press

Key Words: finite simple groups; subgroup chains; rank.

[1] Partially supported by a grant from the NSF.
[2] Partially supported by a grant from the NSA.

0021-8693/00 $35.00

1. INTRODUCTION

Let $\mathcal{S}$ be the set of finite simple groups; that is, $\mathcal{S}$ is a countable set containing exactly one representative for each isomorphism class of finite simple groups. There are various measures of the complexity of an element $S \in \mathcal{S}$. The most elementary is the order $|S|$ of S. Of course, it has the property that, for each constant C, the set

$$\{S \in \mathcal{S} : |S| \leq C\}$$

is finite. A different measure of the complexity, more closely related to the structure of S, is the length $l(S)$ of the longest chain of subgroups of S. This function gives a better measure of the complexity of S for many computational problems. It has been studied widely [2–4, 7, 9–11].

This short note was inspired by a question of Guido Mislin: Does there exist an infinite set $A \subseteq \mathcal{S}$ of non-abelian finite simple groups and a positive integer N such that $l(G) \leq N$ for all $G \in A$? The answer to this question is, "Yes." In fact, we prove the following more detailed result.

THEOREM A. *Let r be any positive integer. Then there exists an infinite set $\mathcal{A} \subseteq \mathcal{S}$ and a bound N such that for each $S \in \mathcal{A}$, S is a finite simple group of Lie type of Lie rank r and $l(S) \leq N$.*

Note that for the alternating groups, trivially $l(A_n) \geq n - 1$ for all $n \geq 4$ and so no such infinite set can be found among the alternating and sporadic simple groups. If $\mathcal{S}$ consists of groups of Lie type, then N will bound both the field size exponent and the Lie rank. For if $L = L_r(q)$ is a group of Lie type of Lie rank r defined over a field of cardinality $q = p^m$, p prime, and if U is a Sylow p-subgroup of L, then $l(L) > l(U) \geq rm$. Suppose N and M are positive integers and that we have a set $\mathcal{A} \subseteq \mathcal{S}$, such that for every $S \in \mathcal{A}$ we have that $l(S) \leq N$ and S has characteristic at most M (or S is an alternating or sporadic simple group). The above remarks together with the classification of finite simple groups show that then $\mathcal{A}$ is finite. Thus the only way $\mathcal{A}$ can become infinite is by letting the set of characteristics run through an infinite set of primes.

Certain group theoretical conditions on a simple group S are related to the characteristic of S (when S is of Lie type). One such condition is that of S being of weak characteristic 2-type, which roughly picks out the simple groups of Lie type in characteristic 2. (See Definition 3.1 below.) We obtain the following result by an elementary proof without the use of the classification of finite simple groups. It plainly implies, in the notation of the previous paragraph, that for $\mathcal{A}$ as in Theorem A, only finitely many $S \in \mathcal{A}$ are of weak characteristic 2-type. We denote by $\exp_2(n)$ the exponent of 2 in the 2-part of n.

THEOREM B. *There is a function* $g_2: \mathbf{N} \to \mathbf{N}$ *such that if* G *is a finite group of weak characteristic* 2*-type, then we have*

$$|G| \leq g_2(\exp_2(|G|)) \leq g_2(l(G)).$$

The function $l(S)$ is closely connected to the number theoretical function Ω. Recall that $\Omega(n)$ is the number of primes dividing the positive integer n, counting multiplicity. We show in Proposition 2.2 below that $l(S) \leq \Omega(|S|) \leq l(S)^2$. Hence, for any subset $A \subseteq \mathcal{S}$, the set $\{l(S) : S \in A\}$ is bounded if and only if the set $\{\Omega(|S|) : S \in A\}$ is bounded. The main ingredient in the proof of Theorem A is the following purely number theoretic result.

THEOREM C. *For each positive integer* n*, there exist an infinite set* P *of primes and a positive integer* N *such that* $\Omega(p^n - 1) \leq N$ *for all* $p \in P$.

For specific small values of n, one may give explicit values for the upper bound N that permits an infinite set P of primes such that $\Omega(p^n - 1) \leq N$. For example, when $n = 2$, we obtain that N can be taken to be 21. (See Corollary 4.2 below.) This implies that, in answer to Mislin's question, we have the following.

COROLLARY D. *There exist an infinite number of non-isomorphic finite non-abelian simple groups* S *such that* $l(S) \leq 20$*. More precisely, there exist infinitely many primes* p *such that* $l(\mathrm{PSL}(2, p)) \leq 20$.

Presumably, smaller values of N should also be possible, but finding them would require a more elaborate number theoretic analysis.

2. COMPARING $l(S)$ AND $\Omega(|S|)$

LEMMA 2.1. *Theorem C implies Theorem A.*

Proof. Let r be any positive integer. Set $n = r + 1$, and let p be a prime number. Then the group $\mathrm{PSL}(n, p)$ is almost always a finite simple group of Lie rank r. Set $n_0 = n!$. By Theorem C, there exist an infinite set P of primes and a positive integer N such that $\Omega(p^{n_0} - 1) \leq N$ for all $p \in P$. Since $p^i - 1$ divides $p^{n_0} - 1$ for $i = 1, \ldots, n$, it follows directly from the formula for the order of $\mathrm{PSL}(n, p)$ that

$$\Omega(|\mathrm{PSL}(n, p)|) \leq nN + \binom{n}{2}.$$

Set A to be the set of all simple groups of the form $\mathrm{PSL}(n, p)$, where $p \in P$. Then $A \subseteq \mathcal{S}$, A is infinite, and for each $S \in A$ we have $l(S) \leq \Omega(|\mathrm{PSL}(n, p)|) \leq nN + \binom{n}{2}$. Hence, Theorem A holds, as desired.

On the other hand, although $l(G)$ does not bound $|G|$ for non-abelian simple groups G of any Lie rank, $l(G)$ does bound $\Omega(|G|)$ for all finite groups G.

PROPOSITION 2.2. *There is a superadditive function* h: $\mathbf{N} \to \mathbf{N}$ (*i.e.*, $h(a+b) \geq h(a) + h(b)$ *for all* a, b) *such that for all finite groups* G, $\Omega(|G|) \leq h(l(G))$. *In fact, we may take* $h(n) = n^2$.

Proof. Suppose such an h exists for all simple groups G. If G is a finite group with composition factors $\{G_i\}$, then

$$l(G) = \Sigma_i(l(G_i)) \qquad \text{and} \qquad \Omega(|G|) = \Sigma_i(\Omega(|G_i|))$$

and so

$$h(l(G)) \geq \Sigma_i(h(l(G_i))) \geq \Sigma_i(\Omega(|G_i|)) = \Omega(|G|),$$

as claimed.

Thus it suffices to show that $h(n) = n^2$ works for all finite simple groups G. Suppose, by way of contradiction, that this is not the case. Let G be a finite group of minimum order such that $\Omega(|G|) > l(G)^2$. By the previous paragraph, G is a simple group. Let 2^a be the order of a Sylow 2-subgroup of G. Since a Sylow 2-subgroup is a proper nilpotent subgroup of G, we have $a < l(G)$. If G is a sporadic simple group or the Tits group, it is straightforward to check that $\Omega(|G|) \leq a^2$. Hence, G is not a sporadic simple group or the Tits group.

Suppose $G = A_n$ is an alternating group. Then $\Omega(|G|) \leq a\omega(|G|)$, where $\omega(m)$ denotes the number of distinct prime divisors of m. Since, in this case, $\omega(|G|) \leq a + 1$, it follows that $\Omega(|G|) \leq a(a+1) < l(G)^2$, a contradiction. Hence, by the classification of finite simple groups, G is a group of Lie type.

We set $l = l(G)$. Suppose G has proper subgroups H, T_1, T_2, and T_3 such that H is a parabolic subgroup; T_1, T_2, and T_3 are solvable; and $|G|$ divides $|H|\,|T_1|\,|T_2|\,|T_3|$. Then, by induction, since H has a non-trivial normal solvable subgroup, we have $\Omega(|H|) \leq (l-2)^2 + 1$. It follows that

$$\Omega(|G|) \leq (l-2)^2 + 1 + 3(l-1) = l^2 + 2 - l \leq l^2.$$

Hence, such H, T_1, T_2, and T_3 do not exist. If $G \simeq PSL(n, q)$, we may take H to be a parabolic subgroup containing $SL(n-1, q)$ and T_1 and T_2 to be Singer cycles of G and $GL(1, q)$. If $G \simeq PSU(n, q)$, we may take H to be a parabolic subgroup containing $SU(n-2, q)$, and T_1, T_2, and T_3 to be Singer cycles of $PSU(n, q)$, of $GL((n-1)/2, q) \leq SU(n-1, q)$, and of $Sp(n-1, q) \leq SU(n-1, q)$ if n is odd, and T_1, T_2, and T_3 to be Singer cycles of $PSp(n, q) \leq PSU(n, q)$, of $SU(n-1, q)$, and of $GL(n/2, q)$ if n

is even. If $G \simeq PSp(2n, q)$, we may take H to be a parabolic subgroup containing $Sp(2n-2, q)$, and T_1 and T_2 to be Singer cycles of $PSp(2n, q)$ and $GL(n, q)$. If $G \simeq P\Omega(2n+1, q)$, we may take H to be a parabolic subgroup containing $\Omega(2n-1, q)$ and T_1 and T_2 to be Singer cycles of $GL(n, q) \leq \Omega^+(2n, q)$ and $\Omega^-(2n, q)$. If $G \simeq P\Omega^+(2n, q)$, we may take H to be a parabolic subgroup containing $\Omega^+(2n-2, q)$ and T_1 to be a Singer cycle of $GL(n, q)$ and T_2 to be a Singer cycle of $\Omega^-(2n-2, q)$. If $G \simeq P\Omega^-(2n, q)$, we may take H to be a parabolic subgroup containing $\Omega^-(2n-2, q)$ and T_1 to be a Singer cycle of $P\Omega^-(2n, q)$ and T_2 to be a Singer cycle of $GL(n-1, q)$. Hence, G is not a classical group.

Assume there exist a Sylow p-subgroup P and solvable subgroups $T_1, \ldots, T_\alpha$ of G, for some α, such that the order of G divides $|P|\,|T_1| \cdots |T_\alpha|$. Then, we have

$$\Omega(G) \leq (\alpha + 1)(l - 1).$$

Hence, as G is a counterexample, we must have $\alpha > l$.

Since we have eliminated all of the other cases, G is now some exceptional group of Lie type in characteristic p. Let $\overline{G}$ be the corresponding algebraic group and let F be the corresponding Frobenius map. We let, as usual, q be the absolute value of the eigenvalues of the action of F on the character group of a maximally split F-invariant torus. Every element of G of order prime to p is contained in some maximal F-stable torus of $\overline{G}$. By Proposition 3.3.5 in [5], the order of the fixed points T^F of this maximal torus under F is a polynomial $P(q)$ in q with rational coefficients. Suppose first that q is rational. Then, $P(q)$ is actually a divisor of the order of G when viewed in the ring of polynomials in one variable over the integers. Let α be the number of irreducible polynomial factors of the p'-part of the order of G counting multiplicities. Then, there exist a Sylow p-subgroup P and tori $T_1, \ldots, T_\alpha$ of G such that the order of G divides $|P|\,|T_1| \cdots |T_\alpha|$. It follows that $\alpha > l$. On the other hand, the exponent of the order of a Sylow p-subgroup of G provides a lower bound for $l - 1$. This yields a contradiction in every case.

Hence, q is not rational. Writing $q = q_0\sqrt{p}$, we get that the order of the tori of G are divisors of the order of G when viewed as polynomials in q_0 with coefficients in $\mathbf{Q}(\sqrt{p})$. One can see that the number of tori needed is at most 4 for ${}^2B_2(q)$, at most 5 for ${}^2G_2(q)$, and at most 12 for ${}^2F_4(q)$. Comparing again with the orders of the Sylow p-subgroup eliminates the case ${}^2F_4(q)$ as we know that $q \geq 2\sqrt{2}$. Hence, we are left with the cases ${}^2B_2(q)$ and ${}^2G_2(q)$. However, considering the smallest member of these families, we note that $l \geq 8$ for ${}^2B_2(q)$ and $l \geq 29$ for ${}^2G_2(q)$. This final contradiction concludes the proof of the proposition.

3. ELEMENTARY PROOF OF THEOREM B

In this section, we prove Theorem B without using the classification of finite simple groups.

DEFINITION 3.1. We say that a finite group G is of weak characteristic 2-type if, for every 2-subgroup S of G, we have that $O_{2'}(C_G(S)) = 1$.

Although the concept of weak characteristic 2-type may be new to this paper, it is closely related to certain other concepts which are central to the proof of the classification of the finite simple groups. For example, an important subcase of the classification proof is the classification of finite simple groups of characteristic 2-type. G is said to be of characteristic 2-type if $F^*(H)$ is a 2-group for every 2-local subgroup H of G, where $F^*(H)$ is the generalized Fitting subgroup of H. In particular, this implies that $O_{2'}(H) = 1$ for all 2-locals H. Thus any such G is of weak characteristic 2-type. In particular, all of the so-called quasi-thin finite simple groups are of weak characteristic 2-type.

We shall give an elementary proof of Theorem B. We proceed in a short sequence of lemmas.

LEMMA 3.2. *Let G be a finite group of weak characteristic 2-type. If H is the centralizer of a 2-subgroup of G, then H is also of weak characteristic 2-type. Also, if Z is a 2-subgroup of $Z(G)$, then G/Z is of weak characteristic 2-type.*

Proof. Note that if S is a 2-subgroup of G, then $O_{2'}(N_G(S)) = O_{2'}(C_G(S))$.

Let $H = C_G(R)$ for some 2-subgroup R of G. Let S be a 2-subgroup of H and let $X = O_{2'}(C_H(S))$. Note that $C_H(S) = C_G(RS)$ and so $X = 1$. Thus H is of weak characteristic 2-type.

Next let Z be a 2-subgroup of $Z(G)$ and let S be a 2-subgroup of G containing Z. Now $N_{G/Z}(S/Z) = N_G(S)/Z$ and so the preimage in G of $O_{2'}(N_{G/Z}(S/Z))$ is $X = Y \times Z$, where $Y \cong X/Z = O_{2'}(N_G(S)/Z)$. Hence $Y \leq O_{2'}(N_G(S)) = O_{2'}(C_G(S)) = 1$. Hence G/Z is of weak characteristic 2-type.

THEOREM 3.3 (Brauer–Fowler Theorem). *Let $f(x) = (x^2)!$ for $x \in \mathbf{N}$. If $G \neq 1$ is a finite group with $O_{2'}(G) = 1$, then there exists an involution t of G with $|G| \leq f(|C_G(t)|)$.*

Proof. We shall reduce this statement to the more traditional version of the Brauer–Fowler Theorem which asserts that for L a finite simple group

with an involution t such that $|C_G(t)| = c$, we have

$$|L| < \frac{c(c+1)}{2}!$$

(See Corollary(2I) in [1].)

Let N be a minimal normal subgroup of G. As $O_{2'}(G) = 1$, N is a direct product of simple groups of even order. We may choose an involution t in one of these direct factors, L, and set $2 \leq |C_L(t)| \leq |C_G(t)| = c$. By the traditional Brauer–Fowler Theorem it follows that $|L| < (c(c+1)/2)!$. By the structure of characteristically simple groups, every G-conjugate of t in $N - L$ commutes with t, and so

$$|G| = c|t^G| < c(|L| + c) < c\left(\frac{c(c+1)}{2}! + c\right) \leq (c^2)!,$$

as claimed.

Now define g_2: $\mathbf{N} \to \mathbf{N}$ recursively by $g_2(0) = 1$ and $g_2(n+1) = (4g_2(n)^2)!$

LEMMA 3.4. *Let G be a finite group of weak characteristic 2-type. Then* $|G| \leq g_2(\exp_2(|G|))$.

Proof. Suppose not and let G be a counterexample with $\exp_2(|G|)$ minimal. If $|G|$ is odd, then $G = 1$ and the result holds. Hence G contains an involution. By the Brauer–Fowler Theorem we may choose an involution t in G such that $|G| \leq (c^2)!$, where $c = |C_G(t)|$. Let $|G|_2 = 2^{n+1}$, $n \geq 0$. Then by Lemma 3.2, $H = C_G(t)/\langle t \rangle$ is of weak characteristic 2-type with $|H|_2 \leq 2^n$. By induction $|H| \leq g_2(n)$. Thus $c \leq 2g_2(n)$ and $|G| \leq (4g_2(n)^2)! = g_2(n+1)$, as claimed.

Theorem B is an immediate consequence of Lemma 3.4. As a corollary we note the following fact.

PROPOSITION 3.5. *Let G be a finite group all of whose non-abelian simple composition factors are of weak characteristic 2-type. If $l(G) = n$, then* $\Omega(|G|) \leq n \log_2(g_2(n))$.

Proof. If $n = 0$, then $G = 1$ and $\Omega(|G|) = 0 = 0 \cdot \log_2(g_2(0))$. Thus we may assume that $n > 0$. If S is an abelian composition factor of G, then $\Omega(|S|) = 1 \leq \log_2(g_2(n))$, since $n > 0$. Finally, let S be a non-abelian simple composition factor of G. Then, by Lemma 3.4, $|S| \leq g_2(l(S)) \leq g_2(n)$. Now $|S| \geq 2^{\Omega(|S|)}$ and so

$$\Omega(|S|) \leq \log_2(|S|) \leq \log_2(g_2(n)).$$

Thus $\Omega(|G|) \leq m \log_2(g_2(n))$ where m is the number of composition factors of G. As $m \leq n$, we are done.

Clearly, by using Proposition 3.5 we may reduce the proof of Proposition 2.2 to a check for finite simple groups which are not of weak characteristic 2-type. These groups are a subset of the set of "pump-ups" of finite unbalanced simple groups, which were classified in the course of the proof of the Unbalanced Group Theorem. (See [8] for a discussion.) Thus we have the small satisfaction of knowing that Proposition 2.2 relies not on the entire Classification Theorem but only on about 2/3 thereof.

A final comment in this section is that the analogue of the Brauer–Fowler Theorem is known to be true for all primes p, although this is established only after the fact of the Classification Theorem. Clearly we may define groups of weak characteristic p-type for all primes p by analogy with Definition 3.1, and the arguments in Lemmas 3.2 and 3.4 go through, mutatis mutandis, using the function g_p defined recursively by $g_p(0) = 1$ and $g_p(n+1) = (p^2 g_p(n)^2)!$. Thus, as a corollary of the Classification Theorem, we obtain the following analogue of Theorem B.

THEOREM B_p. *There is a function* $g_p\colon \mathbf{N} \to \mathbf{N}$ *such that if* G *is a finite group of weak characteristic* p*-type, then we have*

$$|G| \leq g_p(\exp_p(|G|)) \leq g_p(l(G)).$$

Moreover, every finite simple group of Lie type in characteristic p is of weak characteristic p-type. Thus the fallacy of the analogue of Theorem B for the family of all simple groups is a consequence of the fact that there is no universal bounding function g which works for all primes p.

4. NUMBER THEORY

In this section we prove the number theoretical results that we need. We use standard sieve methods to obtain our results. We begin the proof of Theorem C by setting up some notation. We use the notation of [6] whenever possible. In particular, we denote by $\nu(d)$ the number of prime divisors of the square-free integer d (which, following the Hardy and Wright notation followed by most articles on the function $l(G)$, we had denoted by $\omega(d)$ earlier in the paper). This way we can use ω to define a specific function needed in our case. We refer the reader to [6] for unexplained notation. With the notation in place, we can state Lemma 4.1, which is a more precise version of Theorem C.

Proof of Theorem C. Fix some positive integer n. Let $\overline{\mathfrak{P}}$ be the set of primes p such that $p-1$ divides n. Then $\overline{\mathfrak{P}}$ is a finite set. Let $p \in \overline{\mathfrak{P}}$. Let $m = f_0(p)$ be the smallest positive integer m such that the exponent of the multiplicative group $(\mathbf{Z}/p^m\mathbf{Z})^\times$ does not divide n. We then select some integer $f_1(p)$ relatively prime to p such that p^m does not divide $f_1(p)^n - 1$.

We set $k = \prod_{p \in \overline{\mathfrak{P}}} p^{f_0(p)}$. For each (large) real number x, we introduce the set $\mathscr{A} = \mathscr{A}(x)$,

$$\mathscr{A} = \{p^n - 1 : p \text{ is a prime, } p \le x, \text{ and, for all } q \in \overline{\mathfrak{P}},$$
$$p \equiv f_1(q) \pmod{q^{f_0(q)}}\}.$$

We have chosen $\mathscr{A}$ such that, whenever $a \in \mathscr{A}$, for each $q \in \overline{\mathfrak{P}}$, we have that $q^{f_0(q)}$ does not divide a. We set X to be the following function of x:

$$X = li(x) \cdot \prod_{q \in \overline{\mathfrak{P}}} \frac{1}{\phi(q^{f_0(q)})} = \frac{li(x)}{\phi(k)},$$

where ϕ denotes the Euler function and

$$li(x) = \int_2^{\max(2, x)} \frac{dt}{\log(t)}$$

is the logarithmic integral of x.

We will be sieving the set $\mathscr{A}$ with respect to $\mathfrak{P}$, the set of all primes which are not in $\overline{\mathfrak{P}}$. To this end, for each $z \ge 2$, we set

$$S(\mathscr{A}; \mathfrak{P}, z) := |\{a \in \mathscr{A} : \text{ if } p \in \mathfrak{P} \text{ and } p < z, \text{ then } p \not| a\}|.$$

Our goal is to apply Theorem 7.4, on page 219 of [6]. In order to do so, we need to check the hypotheses denoted by (Ω_1), $(\Omega_2(\kappa, L))$, and $(R(\kappa, \alpha))$ in [6].

Condition (Ω_1) (see page 29 of [6]) says that, for each prime p, we should have

$$0 \le \frac{\omega(p)}{p} \le 1 - \frac{1}{A_1}.$$

In our case, for $p \in \mathfrak{P}$, we have $\omega_0(p) = (\rho(p)/(p-1))p$, where $\rho(p)$ is the number of solutions of

$$y^n - 1 \equiv 0 \pmod{p}.$$

(See (1.3.51) in [6].) Since $\rho(p) < p - 1$ by our choice of $\mathfrak{P}$, and $\rho(p) \le n$, this implies that $0 \le \omega_0(p) \le 1 - 1/A_1$ for all $p \in \mathfrak{P}$, for an appropriate positive A_1. It then follows, by the definition of ω (see (4.12) on page 28 in [6]), that (Ω_1) holds.

Condition $(\Omega_2(\kappa, L))$ appears on page 142 of [6]. We set κ to be the number of divisors of n. Hence, $x^n - 1$ is a product of κ distinct irreducible polynomials. Therefore, by (1.3.17) in [6], we see that

$$\left| \kappa \log(x) - \sum_{p < x} \frac{\rho(p)}{p} \log(p) \right|$$

is bounded. Furthermore,

$$\left| -\sum_{p<x} \frac{\rho(p)}{p} \log(p) + \sum_{p<x} \frac{\rho(p)}{p-1} \log(p) \right| = \sum_{p<x} \frac{\rho(p)\log(p)}{p(p-1)}$$

is also bounded, as is

$$\sum_{p \in \overline{\mathfrak{P}},\ p<x} \frac{\rho(p)}{p-1} \log(p).$$

It then easily follows that

$$-L \le \sum_{w \le p < z} \frac{\omega(p)\log(p)}{p} - \kappa \log\left(\frac{z}{w}\right) \le A_2 \qquad \text{if } 2 \le w \le z, \quad (\dagger)$$

where L and A_2 are appropriate constants depending on n. Hence, $(\Omega_2(\kappa, L))$ holds.

By (1.4.15), (1.3.52), and (1.3.55) in [6], we have

$$|R_d| \le n^{\nu(d)}(E(x, dk) + 1) \qquad \text{if } \mu(d) \ne 0,$$

where μ is the Möbius function, and

$$E(x,k) = \max_{\substack{1 \le l \le k \\ (l,k)=1}} \left| |\{p \le x : p \equiv l \pmod k\}| - \frac{li(x)}{\phi(k)} \right|$$

is the maximal error term in the Prime Number Theorem for arithmetic progressions modulo k. Bombieri's deep theorem concerning these error terms appears as Lemma 3.5 in [6]. Now using Lemma 3.5 (with $U_1 = \kappa + 3$, $h = 3n$, $k = k$, $C = C_1(\kappa + 2, 3n, A)$), and Lemma 3.4 in [6], we obtain

$$\sum_{d < X^{1/2}/\log^{C_1}(X)} \mu^2(d) 3^{\nu(d)} |R_d| \ll \frac{x}{\log^{\kappa+2}(x)} \ll \phi(k) \frac{X}{\log^{\kappa+1}(X)}.$$

Thus, Condition $(R(\kappa, \alpha))$, which appears on page 219 of [6], holds with $\alpha = 1/2$.

We may now apply Theorem 7.4 in [6]. Note however, that the second inequality in the statement of the theorem is reversed due to a misprint. We obtain that, if

$$z^2 \le \frac{X^\alpha}{(\log(X))^{A_4}},$$

then we have

$$S(\mathcal{A}; \mathfrak{P}, z) \ge XW(z)\left\{1 - \eta_\kappa\left(\alpha \frac{\log(X)}{\log(z)}\right) - B_{15} \frac{L(\log\log 3X)^{3\kappa+2}}{\log(X)}\right\}, \quad (*)$$

where

$$W(z) = \prod_{\substack{p \in \mathfrak{P} \\ p<z}} \left(1 - \frac{\omega(p)}{p}\right).$$

By page 212 in [6], η_κ is a strictly decreasing function and there is a unique real number ν_κ such that $\eta_\kappa(\nu_\kappa) = 1$. Hence, for each $u > \nu_\kappa$, we have $\eta_\kappa(u) < 1$. With this notation we can state the next lemma. This lemma obviously implies Theorem C.

LEMMA 4.1. *There exist arbitrarily large primes P such that*

$$\Omega(P^n - 1) \leq \left\lfloor \frac{n\nu_\kappa}{\alpha} \right\rfloor + \sum_{p \in \overline{\mathfrak{P}}} (f_0(p) - 1).$$

Proof. By the discussion above, we know that (Ω_1), $(\Omega_2(\kappa, L))$, and $(R(\kappa, \alpha))$ of Theorem 7.4 in [6] hold. Set

$$\epsilon = \frac{1 + \lfloor n\nu_\kappa/\alpha \rfloor - n\nu_\kappa/\alpha}{3n} > 0.$$

We then consider only such x and z that the relation

$$\frac{\nu_\kappa}{\alpha} + \epsilon = \frac{\log(X)}{\log(z)} \qquad (**)$$

holds. Obviously, for arbitrarily large values of x there will be a corresponding value of z, and as x goes to infinity so does z. Since $\epsilon > 0$, we get that

$$\alpha \frac{\log(X)}{\log(z)} > \nu_\kappa.$$

Taking exponentials, we obtain $z^{\nu_\kappa/\alpha} < X$, so that $z^2 < X^{2\alpha/\nu_\kappa}$. By (4.11) on page 213 of [6], $\nu_\kappa > 2$, so that $2\alpha/\nu_\kappa < \alpha$, and it follows that

$$z^2 \leq \frac{X^\alpha}{(\log(X))^{A_4}}$$

holds for all sufficiently large x. Hence, we may apply Theorem 7.4 in [6] to our situation for all x sufficiently large. Note that

$$\lim_{X \to \infty} B_{15} \frac{L(\log\log 3X)^{3\kappa+2}}{\log(X)} = 0.$$

Since $\alpha \log(X)/\log(z) > \nu_\kappa$, we have that $\eta_\kappa(\alpha \log(X)/\log(z)) < 1$. Hence, the inequality (*) yields

$$\lim_{x \to \infty} (S(\mathcal{A}; \mathfrak{P}, z)) = \infty.$$

Let x be so large that

$$\frac{2\log\log(x)}{\log(z)} = \frac{2\log\log(x)}{\log(X)}\left(\frac{\nu_\kappa}{\alpha} + \epsilon\right) < \epsilon \qquad \text{and} \qquad \frac{\log(\phi(k))}{\log(z)} < \epsilon.$$

Since $X = li(x)/\phi(k)$, the above inequalities hold for all sufficiently large x. Clearly,

$$\frac{x}{\log^2(x)} \leq li(x) \qquad \text{for } x \geq e.$$

Hence, by (**), we have

$$\frac{\log(x/(\phi(k)\log^2(x)))}{\log(z)} \leq \frac{\log(X)}{\log(z)} = \frac{\nu_\kappa}{\alpha} + \epsilon.$$

It follows that

$$\frac{\log(x)}{\log(z)} \leq \frac{\nu_\kappa}{\alpha} + \epsilon + \frac{2\log\log(x)}{\log(z)} + \frac{\log(\phi(k))}{\log(z)} \leq \frac{\nu_\kappa}{\alpha} + 3\epsilon.$$

It follows by our choice of ϵ that

$$\frac{\log(x^n)}{\log(z)} \leq \left\lfloor \frac{n\nu_\kappa}{\alpha} \right\rfloor + 1.$$

We know that the number of elements in the set

$$\{a \in \mathcal{A} : \text{ if } p \in \mathfrak{P} \text{ and } p < z \text{ then } p \nmid a\}$$

becomes arbitrarily large, as x becomes large. Let a be any element of this set. We know that $a = p^n - 1$, for some prime $p \leq x$. Hence,

$$\frac{\log(a)}{\log(z)} < \left\lfloor \frac{n\nu_\kappa}{\alpha} \right\rfloor + 1.$$

It follows that the total contribution to $\Omega(a)$ coming from primes in the set $\mathfrak{P}$ is at most $\lfloor n\nu_\kappa/\alpha \rfloor$. It follows that

$$\Omega(a) \leq \left\lfloor \frac{n\nu_\kappa}{\alpha} \right\rfloor + \sum_{p \in \overline{\mathfrak{P}}} (f_0(p) - 1).$$

This completes the proof of the lemma and of Theorem C.

COROLLARY 4.2. *There are infinitely many primes p such that $\Omega(p^2 - 1) \leq 21$.*

Proof. We just need to apply Lemma 4.1 to the case $n = 2$. Indeed, in this case we have $\overline{\mathfrak{P}} = \{2, 3\}$ and $f_0(2) = 4$ and $f_0(3) = 2$. Furthermore, $\alpha = 1/2$, $\kappa = 2$, and $\nu_\kappa = 4.42\ldots$ (see p. 212 in [6]). Hence, there are infinitely many primes p such that

$$\Omega(p^2 - 1) \leq \lfloor 2 \cdot 2 \cdot 4.42 \cdots \rfloor + (4 - 1) + (2 - 1) = 21,$$

as desired.

Proof of Corollary D. Let p be a large prime such that $\Omega(p^2 - 1) \leq 21$. Such primes exist by Corollary 4.2. Then $l(\mathrm{PSL}(2, p)) = \max\{1 + \Omega(p - 1), 1 + \Omega(p + 1)\}$. (See for example [11].) Furthermore, $2 \leq \Omega(p - 1)$ and $2 \leq \Omega(p + 1)$, which imply that $\max\{\Omega(p + 1), \Omega(p - 1)\} \leq 19$. Hence,

$$l(\mathrm{PSL}(2, p)) \leq 20.$$

Since the $\mathrm{PSL}(2, p)$ are non-isomorphic non-abelian finite simple groups for $p > 3$, this concludes the proof of Corollary D.

Remark. If follows from (†) that $W(z) \geq C/\log^\kappa(z)$, for some constant C. Consequently, the sieve inequality (*) implies that the number of primes $p \leq x$ satisfying $\Omega(p^n - 1) \leq N$ is actually $\gg x/(\log^{\kappa+1}(x))$ as $x \to \infty$. This is a quantitative version of Theorem C.

REFERENCES

1. R. Brauer and K. A. Fowler, On groups of even order, *Ann. Math.* **62** (1955), 565–583.
2. D. Brozovic, Subgroup chains in finite groups, *in* "Group Theory, Granville, OH, 1992," pp. 70–81, World Scientific, River Edge, NJ, 1993.
3. D. Brozovic and R. Solomon, On groups of hyperbolic length, *Israel J. Math.* **98** (1997), 61–99.
4. P. Cameron, R. Solomon, and A. Turull, Chains of subgroups in symmetric groups, *J. Algebra* **127** (1989), 340–352.
5. R. Carter, "Finite groups of Lie Type, Conjugacy Classes, and Complex Characters," Wiley, Chichester/New York/Brisbane/Toronto/Singapore, 1993.
6. H. Halberstam and H. E. Richert, "Sieve Methods," Academic Press, London/New York/San Francisco, 1974.
7. G. Seitz, R. Solomon, and A. Turull, Chains of subgroups in groups of Lie type, II, *J. London Math. Soc.* (2) **42** (1990), 93–100.
8. R. Solomon, The $B(G)$-conjecture and unbalanced groups, *in* "Finite Simple Groups II" (M. J. Collins, Ed.), pp. 63–87, Academic Press, New York, 1980.
9. R. Solomon and A. Turull, Chains of subgroups in groups of Lie type I, *J. Algebra* **132** (1990), 174–184.
10. R. Solomon and A. Turull, Chains of subgroups in groups of Lie type III, *J. London Math. Soc.* (2) **44** (1991), 437–444.
11. A. Turull and A. Zame, Number of prime divisors and subgroup chains, *Arch. Math.* **55** (1990), 333–341.